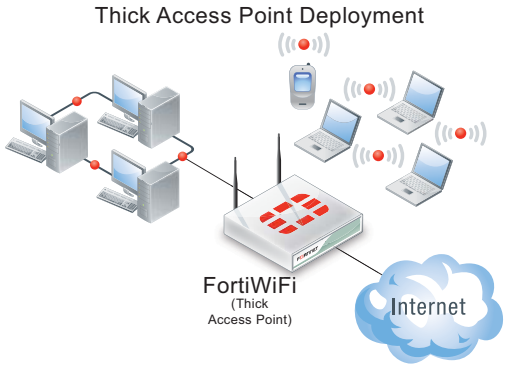
Wireless Networking

FortiGate Wireless Controllers, FortiAP thin access points and FortiWiFi units deliver comprehensive threat management and policy enforcement for wireless networks

A FortiGate unit acting as a FortiGate wireless controller securely integrates wireless networks into your network architecture. Each wireless network or SSID becomes a virtual FortiGate interface that you can apply FortiGate security features to in the same way as a wired interface. FortiGate wireless controllers also include standard and advanced wireless features, including Bring Your Own Device (BYOD) control, wireless IDS (WIDS) and industry standard access control and privacy features that improve security and service availability for wireless users.

How many networks, how many access points?



Using FortiGate wireless features you can create multiple WiFi networks to serve different groups of users. For example, you might want one network for your employees and another for guests or customers. Also, with the increase in use of smartphones, tablets and other mobile devices that use WiFi technology, BYOD wireless networks are becoming more common and busier than ever. Today's wireless networks have to accommodate a very broad range of client devices each with their own strengths and limitations.

FortiGate units support everything from relatively simple single access point wireless networks, to multiple overlapping local wireless networks, and even to remote wireless networks that become virtual extensions of a corporate network. All these networks have vastly different requirements for authentication, access control, and UTM filtering.

In any given location, the number of access points you need depends on the size of the area in which radio coverage is required and the architectural features of the area. You might even need to provide coverage in several different areas, on multiple floors or in multiple buildings or in local and remote locations that may or may not also have wired network access. The number of WiFi networks (SSIDs) you need also depends on the need to separate different kinds of users into different networks.

WiFi Equipment Options

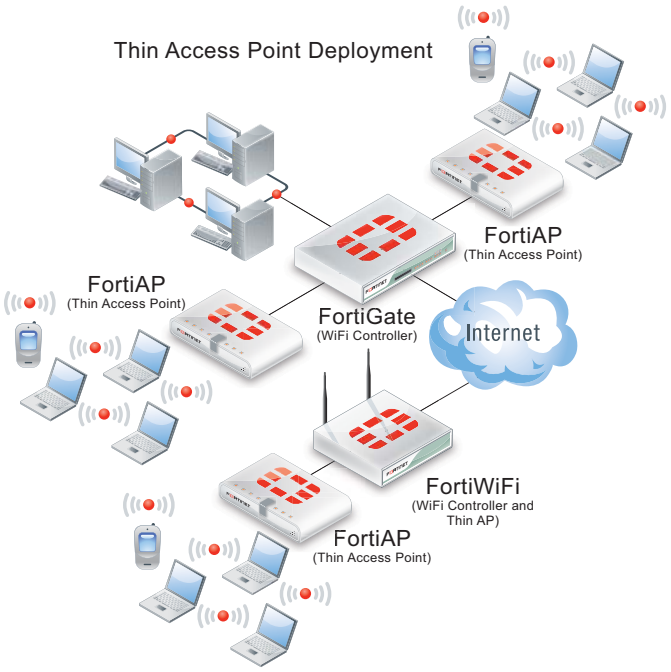
An access point, whether a FortiWiFi or a FortiAP unit, can carry up to eight networks per radio. FortiWiFi access points include one WiFi radio. FortiAP access points include one or two WiFi radios, depending on the model. Each radio can carry up to 8 WiFi networks, seven of these can be user WiFi networks and one is reserved for monitoring.

A network that requires only one WiFi access point is easily created with a FortiWiFi unit operating as a single thick AP. A thick AP such as a FortiWiFi unit contains the WiFi radio and provides access control and authentication.

A thin AP, such as a FortiAP unit contains only the radio and a microcontroller that receives commands and exchanges data with a FortiGate wireless controller. If you already have a FortiGate unit, adding FortiAP units as thin APs managed by your FortiGate unit acting as a FortiGate wireless controller is a cost-effective solution for adding WiFi to your network.

The FortiGate wireless controller feature is available on both FortiGate and FortiWiFi units. A FortiWiFi unit's WiFi controller also controls the unit's internal (Local WiFi) radio facility, treating it much like a built-in thin AP. Whenever multiple APs are required, a single FortiGate or FortiWiFi unit controlling multiple FortiAP units is best.

FortiGate wireless controllers, FortiWiFi units and FortiAP units conform to a number of Control And Provisioning of Wireless Access Points (CAPWAP) specifications, including RFC 4118, RFC 4564, RFC 5418, RFC 5417, RFC 5416, and RFC 5415 and support the 802.11 a, b, g, n and other wireless standards.



Deployment Options

FortiAP units can discover FortiGate wireless controllers through several methods: DHCP, broadcast request, and multicast request. They can also be pre-configured with the controller's IP address. These multiple methods ensure that FortiAP units can communicate with a FortiGate wireless controller even through switches and routers and even across the Internet. The only requirement is to allow traffic on UDP ports 5246 and 5247, used by encrypted CAPWAP tunnels.

The ability to securely tunnel between the FortiAP and the controller over the Internet means travelling users can connect a FortiAP unit configured as a Remote AP to the Internet from a remote location (such as a hotel or conference center) and enjoy direct seamless and secure access to the corporate network.

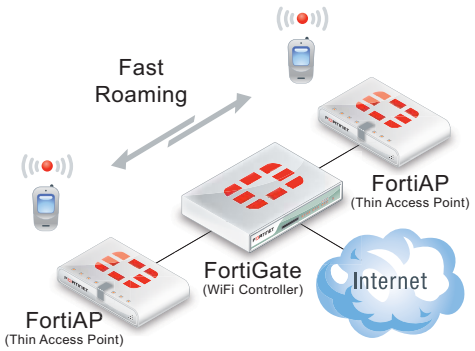
You can also operate a FortiAP in local bridging mode, adding the device to a local internal network. The result is a less complex network configuration because the wired and wireless networks share the same address space and the same FortiOS security configuration. Remote FortiAPs can also operate in local bridging mode, or as separate wireless networks as required.

FortiWiFi and FortiAP units provide adjustable power output of up to 17dBm or 50mW for some models and up to 27dBm or 500mW for others. The output can be optimized to meet or exceed the required power levels to close a two-way communication link with the clients on the wireless network. The actual WiFi signal depends on obstructions and interference sources, but in general for indoor deployments with obstructions a FortiWiFi or FortiAP access point can cover a radius of 50-60 feet (18 meters). To provide a signal for a larger area, FortiAP devices can be deployed every 60 feet in a hexagonal or honeycomb pattern.

To determine optimal deployment scenarios Fortinet's FortiPlanner WiFi planning tool can be used to map the buildings and outdoor locations that you want to add WiFi access to. Then using FortiPlanner you can map out optimal locations for access points and adjust transmitter power settings to provide optimal WiFi coverage.

Fast Roaming

Mobile device users are very likely to move from one AP coverage area to another while communicating. After the mobile user authenticates, the WiFi controller caches the Pairwise Master Key (PMK) to enable the user to associate quickly with other APs in the network, transferring from one AP to another without interruption. This is done in accordance with 802.11i "fast-associate-in-advance" and "fast-roam-back" features.



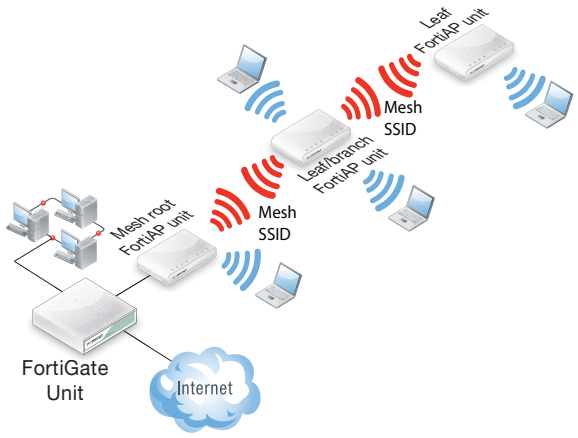
Distributed ARRP (Automatic Radio Resource Provisioning)

In a multi-AP network, adjacent APs need to operate on different radio channels so that they do not interfere with each other. Also, to provide the best service, APs should avoid channels with interference from neighboring APs. By enabling multiple channels when configuring managed FortiAPs, you enable the ARRP algorithm. With ARRP enabled, each AP will re-evaluate its choice of channel at configurable time intervals (for example, every 10 minutes) and change channels if needed to optimize WiFi performance.

Wireless Mesh

FortiAP access points usually communicate with to their wireless controller through Ethernet wiring. A wireless mesh eliminates the need for Ethernet wiring by connecting neighboring FortiAP access points to the controller by radio. This is a useful way to extend a wireless network into an area where installation of Ethernet wiring is impractical.

In a wireless mesh configuration only one FortiAP unit needs to be connected to the Ethernet network. This becomes the root FortiAP unit. Using a dedicated mesh SSID, the root FortiAP unit communicates with branch FortiAP units which relay mesh traffic between the root FortiAP unit and leaf FortiAP units. Root, branch and leaf FortiAP units all also provide wireless access for wireless users.



Wireless client load balancing for high-density deployments

Wireless load balancing allows a wireless network to distribute wireless traffic more efficiently among access points and available frequency bands. FortiGate wireless controllers support access point hand-off and frequency hand-off. Access point hand-off distributes traffic among available access points so that the load is shared equally. Frequency hand-off evenly distributes traffic between the 2.4GHz and 5GHz bands to prevent one from being saturated while the other is under used.

WiFi Security, User Authentication and Device authentication

WiFi security and user authentication controls the authentication methods used by the WiFi network to identify a user before granting access and the encryption and privacy methods used to encrypt data sent over the WiFi network. WiFi security and user authentication can be customized for each WiFi network (SSID).

The FortiOS wireless controller supports standard WPA/WPA2-Personal and WPA/WPA2-Enterprise (802.11i) wireless security modes. Both WPA and WPA2 are supported with AES encryption. TKIP encryption is provided for backward compatibility with WiFi clients that do not support AES encryption.

In addition, FortiOS offers a Captive Portal mode that applies the complete set of user authentication options available for authenticating wireless users. FortiOS user authentication features include RADIUS, LDAP, TACAS+ remote authentication, single sign on (SSO) authentication, and two-factor authentication using FortiToken, certificates, SMS, or email. The messages displayed by the captive portal can be customized, for example to present a disclaimer (usage policy) to which the user must agree before gaining access to the network. Each WiFi network can have its own custom captive portal.

FortiOS device identification and authentication can also be used at the device level to control access to the wireless network. Access can be controlled depending on the device type or by individual device MAC address.

WPA-Enterprise mode can authenticate users with an external RADIUS server (802.1X) or through FortiOS user authentication in which the user must be a member of a specified user group.

FortiGate wireless controllers support white listing or black listing WiFi devices based on MAC address. White listed devices can be granted access without the need for further authentication. Black listed devices can be blocked from even being allowed to authenticate. MAC addresses may also be used to build a local authentication database. All devices not on the white or black lists are subject to the authentication required for the WiFi network.

If there is no reason for clients to communicate directly with each other, security can also be enhanced by enabling intra-SSID privacy that blocks individual users from communicating with each other on the same wireless network. This security enhancement prevents “man in the middle” attacks between wireless client devices.

WiFi Guest access provisioning

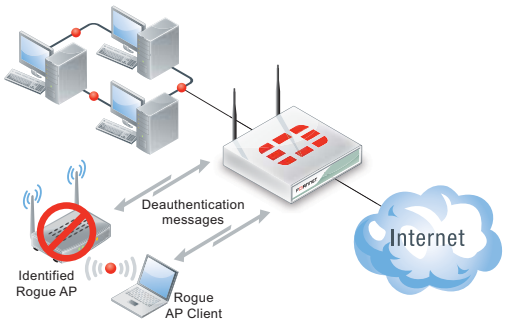
Guest access provisioning allows easy addition of temporary guest accounts to give guest WiFi users temporary access to a WiFi network. Guest account information can be distributed to guest users by printing account information or by sending it in emails or SMS messages.

Many guest account options are available including:

- Email address or user name to identify the guest account
- Requiring a password or no password to log in
- Configurable account expiry time, starting immediately or after the first login
- Batch guest account creation using auto-generated user IDs and passwords

Monitoring Neighbors and Rogues

In almost any WiFi environment, access points other than your own are active. Most of these are neighbors which might cause interference but are not a security threat. Unauthorized APs connected to your networks are rogue APs that can cause leakage of sensitive information to malicious parties. This issue is particularly important if your organization must comply with the Payment Card Industry Data Security Standard (PCI DSS). The FortiOS on-wire detection technique correlates wireless MAC addresses on other APs with those on your wired networks to differentiate neighbors from rogues. FortiOS can generate alert messages to inform system administrators when a rogue AP is identified.



Suppressing Rogues

When activated, suppression against suspected rogue APs sends deauthentication frames to the rogue and its clients. This stops unwanted communication with the rogue AP until it can be found and removed from the network.

Wireless IDS

Wireless IDS (WIDS) monitors wireless traffic for a wide range of security threats by detecting and reporting on possible intrusion attempts. FortiOS WIDS can detect ASLEAP attacks, unauthorized wireless devices, rogue and interfering APs, many forms of flooding, adhoc networks, spoofed de-authentication, and more. Optimum thresholds and intervals can be set for many of these attacks. The default WIDS profile can be used or multiple WIDS profiles can be created for different protection requirements.

IEEE 802.11e and Application-based QoS

In addition to full support for IEEE 802.11e, FortiOS supports application-based Quality of Service control. Business-critical applications can be given preferential treatment over non-essential applications. Fortinet’s unique approach to Quality of Service by supporting both 802.11e and layer 7 application prioritization and traffic shaping provides significant value to enterprise users.